

3

DNS 服务器的配置与管理

【项目导读】

今天我们在 Internet 上浏览各个网站时,通常都使用的是由字母和数字组成的该网站域名,而很少有人直接用 IP 地址去访问。这其中的原因很简单,有意义且生动形象的域名相比较枯燥的 IP 地址更容易被人理解和记忆。例如,当我们要访问新浪网站时,只需要在浏览器的地址栏内输入 `www.sina.com.cn` 即可访问新浪中国网站的主页,而不需要记住该网站的 IP 地址 202.108.33.93。

通过以上的例子我们已经可以了解域名系统的基本功能,但是我们也注意到,实际上在有众多路由器连接而成的 Internet 上,路由器根本不认识和理解我们所使用的域名,而只能机械地接受枯燥的 IP 地址。那么我们是怎么通过简单的域名进行访问的呢?这个问题的答案很简单,那就是有一个系统将我们输入的域名转换为对应的 IP 地址,这种转换我们称之为域名解析,即 DNS 解析,而完成这种转换的设备就是 DNS 服务器。

DNS (Domain Name System, 域名系统)的主要工作是域名解析,也就是把域名翻译成 IP 地址,这样我们就可以直接用易于联想记忆的计算机名来进行网络通信,而不用去记忆那些枯燥晦涩的 IP 地址了。

【教学目标】

1. 理解域名解析系统结构。
2. 理解 DNS 解析过程。
3. 理解 DNS 区域文件记录类型。
4. 理解 DNS 子域基本概念。
4. 掌握 DNS 服务器正反向查找区域配置方法。
5. 掌握辅助 DNS 服务器配置方法。
6. 掌握建立 DNS 子域和子域权限委派配置方法。

3.1 DNS 基本概念与工作原理

任务一 理解 DNS 体系结构

【任务描述】

理解域名解析系统 DNS 的体系结构。

【任务要求】

1. 理解 Hosts 文件作用。
2. 理解 DNS 体系结构。

【知识链接】

1. 域名解析系统的发展史

DNS 是域名解析系统，用于实现将我们输入的域名转换为对应的 IP 地址，进而使用转换后的 IP 地址去访问指定的服务器。这样我们就不需要去记忆枯燥晦涩的 IP 地址了。现在我们思考一个问题，在 DNS 广泛应用之前，Internet 上是如何进行计算机名称解析的呢？这个问题显然是有实际意义的，描述 DNS 的 RFC882 和 883 文档出现在 1984 年，但 1969 年 11 月互联网就诞生了，难道在 DNS 出现之前，互联网的先驱们都是互相用 IP 地址进行通信的？答案当然是否定的，但早期互联网的规模确实非常小，最早互联网上只有 4 台主机，分别在犹他大学、斯坦福大学、加州洛杉矶分校和加州圣芭芭拉分校，即使在整个 20 世纪 70 年代，互联网上也只有几百台主机而已。

这样一来，解决名称解析的问题就可以使用一个非常简单的办法，每台主机利用一个 Hosts 文件，在 Host 文件内记录了当时互联网上的所有主机名称和 IP 地址的映射关系。Hosts 文件是一个完全分散解析方案，每台主机都自己负责名称解析，利用这个 Host 文件就可以把互联网上所有的主机都解析出来。这个 Hosts 文件现在我们还在使用，路径就在 \Windows\System32\Drivers\etc 目录下，如图 3-1 所示就是一个 Hosts 文件的例子，我们在图中可以很清楚地看到 Hosts 文件可以把 www.baidu.com 解析为 202.108.22.5。

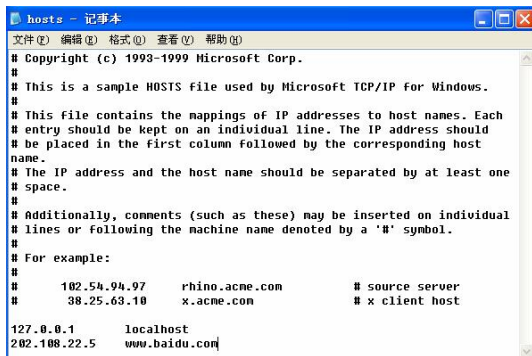


图 3-1 Hosts 文件

显然在一个规模很小的互联网上使用 Host 文件是一个很简单的解决方法，只需要管理员每周下载一次更新后的 Host 文件就可以实现计算机名的解析。但这种方案在 Internet 急剧扩张的今天就不适用了。那么今天的互联网是如何实现解析的呢？

2. 域名解析系统 DNS 的体系结构

互联网的管理者们已经有了一种更成熟的方案,那就是今天的域名解析系统,即 DNS (Domain Names Systems) 系统。DNS 采用有层次结构的名称空间为主机命名(即域名),以确保主机域名的唯一性,目前 DNS 采用的是分布式的解析方案。互联网管理委员会规定,域名空间的解析权都归根服务器所有,也就是说,根服务器对互联网上所有的域名都享有完全的解析权(即由 Internet 域名管理机构 Inter NIC 负责根服务器的管理)。当然这并不意味着根服务器保存着全世界的所有域名解析信息。例如,根服务器把 com 结尾的域名解析权委派给其他的 DNS 服务器,以后所有以 com 结尾的域名就不需要根服务器负责解析了,而由被委派的服务器负责解析。此外,根服务器还把以 net、org、edu、gov 等结尾的域名都一一进行了委派,这些被委派的域名被称为顶级域名,每个顶级域名都有预设的用途,例如 com 域名用于商业公司、.edu 域名用于教育机构、.gov 域名用于政府机关等,这种顶级域名也被称为顶级机构域名。根服务器还针对不同国家进行了域名委派,例如把所有以 CN 结尾的域名委派给中国互联网管理中心,以 JP 结尾的域名委派给日本互联网管理中心,CN、JP 这些顶级域名被称为顶级地理域名。DNS 的这种层次逻辑树结构如图 3-2 所示。

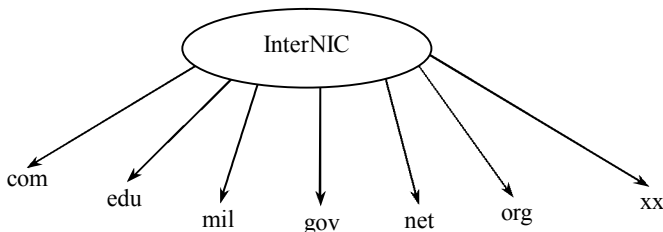


图 3-2 DNS 的顶级域名

同样,每个被委派的 DNS 顶级域名可以按照委派的方式向下进行进一步的委派。例如,要使用 sina.com 域名,就需要向负责.com 域名的 DNS 服务器进行申请。只要该域名没有被其他人使用,在缴纳了相应的费用之后,负责.com 域名的服务器就会把 sina.com 域名委派到新浪公司自己的 DNS 服务器。Sina.com 被称为二级域名。

同理,如果要使用 chongqing.sina.com 子域名,只需要向负责 sina.com 域名的新浪公司 DNS 服务器进行申请。在审查同意之后,负责 sina.com 域名的服务器就会把 chongqing.sina.com 域名委派到重庆新浪公司自己的 DNS 服务器。Chongqing.sina.com 被称为子域名。只要这种委派一级级发展下去,就会形成分层次的逻辑树型结构。

值得注意的是,在二级域名以下就可以创建子域名或者主机名。例如在图 3-3 中,sina.com 以下的 FTP 和 NEWS 是位于 Sina.com 域中的两台主机名。我们前面所谈的域名结构就是主机名+.DNS 后缀=FQDN(完全合格域名)。例如,图 3-3 中位于 sina.com 域内的 FTP 服务器的完全合格域名就是 ftp.sina.com.,NEWS 服务器的完全合格域名就是 news.sina.com.。

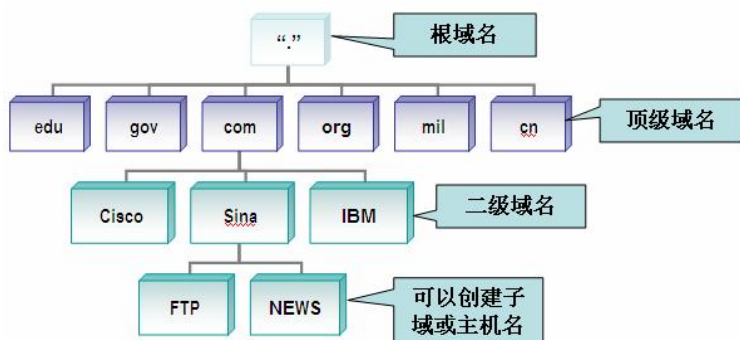


图 3-3 DNS 分层结构

注意：顶级域名 com 之后有一个小圆点，它代表的是根域。对于完全合格域名而言是不能省略这个点的。

任务二 理解 DNS 的解析过程

【任务描述】

理解域名解析系统 DNS 的解析过程。

【任务要求】

1. 理解 DNS 系统查询和响应方式。
2. 理解 DNS 区域及文件记录类型。
3. 理解 DNS 解析过程。

【知识链接】

1. DNS 按照查询方式

DNS 的查询方式分为正向地址解析和反向地址解析。正向地址解析是指 DNS 客户端向 DNS 服务器提交域名查询 IP 地址，或者是 DNS 服务器向另一台 DNS 服务器提交域名查询 IP 地址，被请求的 DNS 服务器作出响应的过程称为正向解析。反之，DNS 客户端向 DNS 服务器提交 IP 地址而查询域名的响应过程被称为反向地址解析。

2. DNS 按照响应方式

根据 DNS 服务器对于 DNS 客户端的不同响应方式，域名解析可以分为递归查询和循环（迭代）查询。

（1）递归查询。

递归查询是指 DNS 客户端发出查询请求后，如果 DNS 服务器内没有所需的数据，则 DNS 服务器会代替客户端向其他 DNS 服务器进行查询。在这种方式中，DNS 服务器必须给 DNS 客户端作出回答。

（2）循环查询（迭代查询）。

循环查询是指每次请求一个服务器，不行再请求其他的服务器。例如请求第 1 台 DNS 服

务器失败,第1台DNS服务器提供第2台DNS服务器发给客户端,客户端再向第2台提出查询请求,如果在第2台内没有所需要的数据,则它会提供第3台DNS服务器的IP地址给客户端,让客户端向第3台DNS服务器进行查询。

3. DNS 的解析过程

我们以一个DNS域名解析的实例来说明DNS的解析过程。例如,现在有一台主机需要查询域名www.163.com的IP地址。整个解析过程如下:

(1) 客户端提出域名解析请求(无论以何种形式或方法),并将该请求发或转发给本地的DNS服务器;

(2) 本地DNS服务器收到请求后就去查询自己的缓存,如果有该条记录,则会将查询的结果返回给客户端。反之,如果DNS服务器本地没有搜索到相应的记录,则会把请求转发到根DNS(13台根DNS服务器的IP信息默认均存储在DNS服务器中,当需要时就会去有选择性地连接);

(3) 某一个根DNS服务器收到请求后会判断这个域名是谁来授权管理,并会返回一个负责该域名子域的DNS服务器地址。比如,查询www.163.com的IP地址,根DNS服务器就会在负责.com顶级域名的DNS服务器中选一个(并非随机,而是根据空间、地址、管辖区域等条件进行筛选),返回给本地DNS服务器。由于根域对顶级域名有绝对管理权,自然也知道他们的全部信息,因此就可以告诉本地DNS服务器负责.com的DNS服务器地址;

(4) 本地DNS服务器收到这个地址后,就开始联系对方并将此请求发给他。负责.com域名的某台DNS服务器收到此请求后,如果自己无法解析,就会返回一个管理.com的下一级的DNS服务器地址给本地DNS服务器,也就是将负责管理163.com的DNS服务器地址告诉本地DNS服务器;

(5) 当本地DNS服务器收到这个回复后,就会重复上面的动作,继续往下联系;

(6) 不断重复这样的轮回过程,直到有一台DNS服务器可以顺利解析出这个地址为止。在这个过程中,客户端一直处于等待状态;

(7) 直到本地DNS服务器获得IP时,才会把这个IP返回给客户端。在本地的DNS服务器取得IP地址后,递归查询就算完成了。本地DNS服务器同时会将这条记录写入自己的缓存,以备后用。到这一步整个解析过程完成。

整个解析过程如图3-4所示。在这个过程中,我们注意到,本地DNS服务器的响应方式就是递归查询,而根服务器、.com和163.com的DNS服务器都是工作在循环(迭代)方式下的。这说明流量大的DNS服务器通常只采用循环(迭代)方式,因为如果它们对每一个解析请求都代为查询(即递归查询方式)的话,那将会消耗极大的服务器资源,可能会导致服务器过载甚至崩溃。

客户端拿到这个解析出来的IP地址后,就可以顺利地对www.163.com进行访问了。但假设客户端请求的域名根本不存在,解析自然不成功,DNS服务器会返回此域名不可达,在客户端的体现就是网页无法浏览或网络程序无法连接等。

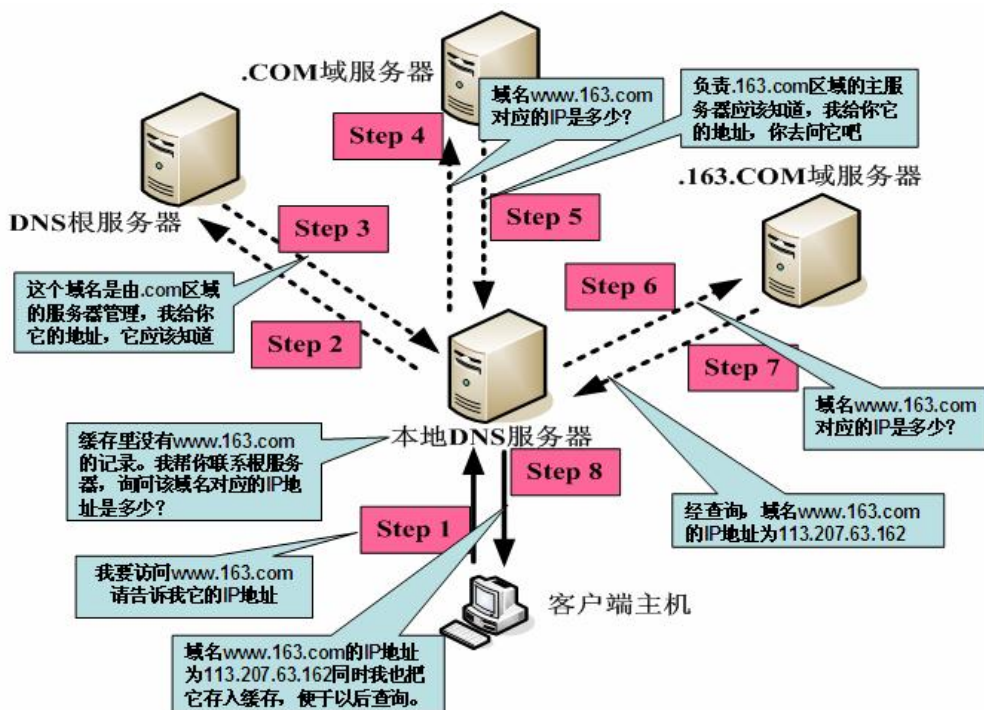


图 3-4 DNS 的完整解析过程

4. DNS 区域及文件记录

DNS 区域简称区域，是域名空间中连续的一部分。DNS 服务器是以区域为单位来管理域名空间的，区域中的数据保存在区域文件中。例如，`www.sina.com` 域名的数据就保存在区域 `sina.com` 中，并由 `sina.com` 来对 `www.sina.com` 域名进行管理。因此 `sina.com` 区域内的主 DNS 服务器就要负责对 `www.sina.com` 域名的解析，在 DNS 服务器中也必须有这样的一个区域文件。

DNS 的区域有三种类型：主要区域、辅助区域和存根区域。通常企业申请域名时都会考虑建立两个 DNS 服务器，一般的解析请求由主服务器负责，辅助服务器的数据是从主服务器复制而来的，辅助服务器的数据是只读的，当主服务器出现故障或由于负载太重无法响应客户机的解析请求时，辅助服务器会担负起域名解析的任务。因此主要区域就是主 DNS 服务器建立的区域，辅助区域就是辅助 DNS 服务器建立的区域，存根区域可以看作是一个特殊的、简化的辅助区域。在 DNS 的区域文件中，常用的记录有以下几种：

(1) A 记录（即主机记录）。

A 记录也称为主机记录，是使用最广泛的 DNS 记录，A 记录的基本作用就是说明一个域名对应的 IP 是多少。例如，如果我们需要建立一个由域名 `ftp.sina.com` 到 IP 地址 `202.96.13.9` 的解析关系，那么就需要在 DNS 区域文件中建立一个 A 记录，实现正向地址解析。简而言之，

DNS 服务器上建立一条 A 记录就是建立起一个由域名到 IP 地址的映射关系。

(2) NS 记录（即名称服务器记录）。

NS 记录和 SOA 记录是任何一个 DNS 区域都不可或缺的两条记录，NS 记录也叫名称服务器记录，用于说明这个区域有哪些 DNS 服务器负责解析；SOA 记录说明负责解析的 DNS 服务器中哪一个是主服务器。因此，任何一个 DNS 区域都不可能缺少这两条记录。例如，如果我们需要区域 test.com 中有两个 DNS 服务器，dns1.test.com 是主 DNS 服务器，IP 地址为 202.96.16.1，dns2.test.com 是辅助 DNS 服务器，IP 地址为 202.96.26.2。那么我们就必须在区域文件中建立两个 NS 记录。

(3) SOA 记录（即起始授权机构记录）。

在 NS 记录中，说明了能够解析本区域的 DNS 服务器有哪些，但 NS 记录并没有说明哪一个服务器是主服务器。SOA 记录中负责说明哪个 DNS 服务器是主服务器，以及主服务器和辅助服务器之间的一些关联参数。

(4) MX 记录（即邮件交换记录）。

MX 记录即 Mail Exchanger，主要用于邮件服务器，作用是定位邮件服务器的地址。如一个用户要给 user@test.com 的用户发封邮件，此时该用户所属的邮件系统会通过 DNS 服务器来查找 test.com 这个域名的 MX 记录，如果存在该记录，就会根据这个 MX 记录来查找对应的 A 记录，从而得到邮件服务器的 IP 地址，并将这封邮件发送到这台服务器上。可见，MX 记录和 A 记录是分不开的。总之，MX 记录是为了让对方找到你的邮件服务器而建立的，所以想顺利接收邮件，就必须为你的邮件服务器创建合法有效的 MX 记录。

(5) CNAME 记录（即别名记录）。

CNAME 记录，即别名记录。我们通过设置别名记录，可以将多个域名指向同一台服务器，相当于给一个人起的外号。比如有台域名为 server.sina.com 的主机上提供邮件和网页服务，我们可以设置 www 和 mail 这 2 个名称的别名记录指向这台服务器，用户可以通过 www.sina.com 和 mail.sina.com 来访问各自需要的服务，但实际上，目标都是同一台服务器。之所以要使用别名记录，主要原因之一在于想让一台服务器扮演多种角色而使用户感觉不到；另外一个原因就是出于安全方面的考虑因素，例如我们不希望别人知道某个网站的真实域名，那我们可以让用户访问网站的别名。

(6) PTR 记录（即指针记录）。

PTR 记录是 A 记录的逆向记录，作用是把 IP 地址解析为域名。由于我们在前面提到过，DNS 的反向区域负责从 IP 到域名的解析，因此如果要实现反向地址解析，必须在反向区域中创建 PTR 记录。

任务三 理解辅助 DNS 服务器子域委派和转发器的工作原理

【任务描述】

DNS 服务器的重要性是不言而喻的，为了防止因主 DNS 服务器故障而导致的网络瘫痪，

就必须设置具有备份功能的辅助 DNS 服务器。

【任务要求】

1. 理解 DNS 辅助服务器工作原理。
2. 理解 DNS 主从服务器区域文件的复制方式。

【知识链接】

1. 设置 DNS 辅助服务器的必要性

对于一个 DNS 区域来说, 实际应用中都不可能只设置一台 DNS 服务器, 因为越来越多的网络应用都依赖于 DNS 解析才能完成。DNS 的重要性是不言而喻的, 甚至可以说 DNS 系统的安全直接决定了网络系统的安全。所以建立一个区域进行域名解析时, 往往都会建立多台 DNS 服务器共同完成。在这众多的 DNS 服务器中有一台扮演主要角色的服务器, 即主 DNS 服务器, 其他的 DNS 都被称为辅助 DNS 服务器。设置 DNS 辅助服务器的优点主要有以下几点:

- 容错能力。

配置辅助服务器后, 在该区域主服务器崩溃的情况下, 客户机的解析请求依然能得到响应。通常主服务器和辅助服务器安装在不同子网上, 这样如果到一个子网的连接中断, DNS 客户机还能直接查询另一个子网上的名称服务器。

- 减少广域网链路的通信量。

如果某个区域被远方的大量客户机访问, 就可以直接在远方网络内设置该区域的辅助服务器, 并把远程客户机配置成先查询这些辅助服务器, 这样就能防止远程客户机通过慢速链路通信来本区域找主 DNS 服务器进行 DNS 查询。

- 减轻主服务器的负载。

辅助服务器能代替主服务器回答该区的查询, 从而减少该区主服务器必须回答的查询数。

2. 主 DNS 服务器和从 DNS 服务器区域文件的同步

主 DNS 服务器保存着区域的所有文件记录, 辅助服务器定期与主服务器进行同步, 从主服务器那里复制区域文件到本服务器上。但出于安全原因, 主服务器并不允许任意的 DNS 服务器从自己的区域中复制数据, 默认情况下, 只有这个区域的 DNS 服务器才被允许成为辅助 DNS 服务器。当然, 我们也可以直接指定允许进行复制的辅助 DNS 服务器名称或 IP 地址。甚至可以允许所有服务器进行复制 (这种方式不推荐采用)。在本例中, 为安全起见, 我们采用默认的仅允许本区域的服务器有复制权限。因此我们就必须在设置辅助服务器之前, 使辅助服务器成为本区域的 DNS 服务器, 取得从主服务器那里复制区域文件的权限。配置应该遵循以下步骤:

- (1) 辅助服务器主机名后面增加后缀, 成为该区域的服务器;
- (2) 在主服务器上增加一条关于辅助服务器的主机记录 (A 记录);
- (3) 在主服务器的 NS 记录中增加该辅助服务器, 即辅助服务器具备复制权限;
- (4) 在主服务器的“文件传递”内选择“仅允许本区域的服务器复制”;

- (5) 辅助服务器上建立正向和反向辅助查找区域;
- (6) 辅助服务器上从主服务器复制区域文件, 实现主从同步。

任务四 理解子域委派和转发器的工作原理

【任务描述】

子域的创建使得 DNS 服务器的管理趋于复杂, 为了简化管理设置, 需要将子域的域名解析任务委派给子域内的 DNS 服务器。同时当 DNS 服务器无法解析域名请求时, 也需要采用转发器的方式转发解析请求。

【任务要求】

1. 理解子域及子域权限委派的工作原理。
2. 理解 DNS 转发器的工作原理。

【知识链接】

1. DNS 子域和子域委派的基本概念

如前所述, DNS 是按照分层思想组织的逻辑结构。每一个 DNS 层次都可以发展下一级的子域。例如在区域 `cnnnet.com.cn` 中创建子域 `sh.cnnnet.com.cn`, 表示上海分公司的域名。但是区域中的子域过多时维护起来不方便, 并且还会遇到域名查询量的瓶颈。比较好的解决方案就是通过区域中新建委派, 将子域委派到其他服务器维护, 从而有效地减轻了区域域名解析的工作量。例如在区域 `cnnnet.com.cn` 的解析工作量中, 将子域 `sh.cnnnet.com.cn` 的域名解析工作委派给另外的 DNS 服务器负责。

2. DNS 转发器的基本概念和工作原理

在前面内容的学习中, 我们知道本地 DNS 服务器遇到无法解析的域名时, 会将解析请求发送给根服务器。其实本地 DNS 服务器除了向根服务器寻求帮助外, 还可以通过设置转发器来转发域名解析请求。通常当 DNS 服务器在收到 DNS 客户端的查询请求后, 它将在所管辖区域的数据库中查找是否有该客户端的解析数据。如果该 DNS 服务器的区域数据库中没有该客户端的数据 (即在 DNS 服务器所管辖的区域数据库中并没有该 DNS 客户端所查询的域名), 该 DNS 服务器就会转向其他的 DNS 服务器进行查询, 这种将查询转发给其他 DNS 的服务器就被称为 DNS 转发器。

在实际应用中, DNS 转发器的应用非常普遍。例如, 当网络中的主机要与外网机通信时, 就需要向外界的 DNS 服务器进行域名查询, 并由其提供域名解析数据。但考虑到安全性, 一般不希望内部所有的 DNS 服务器都直接与外界 DNS 服务器建立联系, 而是只让指定的 DNS 服务器与外界建立直接联系, 网络内的其他 DNS 服务器则通过这一台 DNS 服务器来与外界进行间接的联系。有了转发器后, 当 DNS 客户端提出查询请求时, DNS 服务器将通过转发器从外界 DNS 服务器中获得数据, 并将其提供给 DNS 客户端。

3.2 DNS 服务器的基本配置

任务五 DNS 部署规划

【任务描述】

JSGroup 集团是国内机械制造业的知名企业，该企业随着经营业务的发展，已经对电子商务等网络营销模式有了更高的需求，因此该企业加快了信息化建设及管理步伐，建设了企业内部的局域网。购置了多台服务器，其中 Web 服务器一台、电子邮件服务器两台以及企业内部办公自动化 OA 服务器一台、FTP 服务器一台。该企业为了加强对外交流和开展电子营销，专门申请了域名 jsgroup.cn。为了方便用户使用域名方式访问公司服务器，就必须建设 DNS 服务器。

【任务要求】

- 1. 规划 DNS 服务器的 IP 地址。
- 2. 设置各类服务器域名及对应的 IP 地址。

【实施方法】

- 1. 规划 DNS 服务器的域名及地址

由于申请的公网域名为 JSGroup.cn，因此设置 DNS 服务器的主机名为 dns.jsgroup.cn，并且设置 DNS 服务器使用静态 IP 地址 202.168.10.5/24。

- 2. 网络服务器的域名及 IP 地址规划

公司内部的各个服务器所使用的域名及地址设置如下：

- （1）企业的网站服务器使用的域名为www.jsgroup.cn，对应的内网地址为 202.168.10.10/24；
- （2）FTP 服务器的域名为 ftp.jsgroup.cn，对应的内网地址为 202.168.10.20/24；
- （3）OA 服务器的域名为 oa.jsgroup.cn，对应的内网地址为 202.168.10.30/24；
- （4）邮件服务器的域名为 Email.jsgroup.cn，对应的内网地址为 202.168.10.40/24。

以上要求如表 3-1 所示。

表 3-1 DNS 规划表

服务器种类	规划的服务器域名	服务器 IP 地址
DNS 服务器	dns.jsgroup.cn	202.168.10.5/24
网站服务器（Web 服务器）	www.jsgroup.cn	202.168.10.10/24
FTP 服务器	ftp.jsgroup.cn	202.168.10.20/24
OA 系统服务器	oa.jsgroup.cn	202.168.10.30/24
EMAIL 服务器	Email.jsgroup.cn	202.168.10.40/24

任务六 DNS 服务器基本配置

【任务描述】

根据 DNS 部署规划, 要求 DNS 服务器能提供由域名到 IP 地址的解析以及由 IP 地址到域名的解析功能。

【任务要求】

1. 安装 DNS 服务组件。
2. 建立正向查找区域, 实现域名到 IP 解析。
3. 建立反向查找区域, 实现 IP 到域名解析。

【实施方法】

1. DNS 服务器的安装

首先选择一台专业服务器作为 DNS 服务器的硬件平台, 然后在服务器上面安装 Windows Server 2008 操作系统。再设置 DNS 服务器的静态 IP 地址为 202.168.10.5/24。接下来的安装步骤如下:

- (1) 单击“开始”按钮, 选择“管理工具”→“服务器管理”命令, 如图 3-5 所示;
- (2) 在“服务器管理”对话框中单击“角色”选项;
- (3) 在右侧的“角色摘要”内单击“添加角色”→“下一步”按钮, 在出现的“添加角色向导”对话框中勾选“DNS 服务器”复选项, 然后单击“下一步”按钮, 如图 3-6 所示;



图 3-5 打开“服务器管理器”

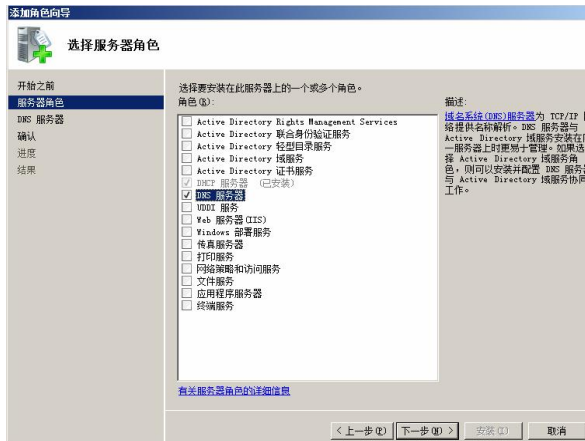


图 3-6 选择 DNS 服务器

- (4) 在“确认”对话框中确定安装 DNS 服务器, 然后单击“下一步”按钮, 开始安装;
- (5) 安装完成之后, 可以在安装结果对话框内看到安装后的结果, 如果提示“安装成功”, 则单击“关闭”按钮, 完成安装。然后单击“开始”→“管理工具”→“DNS”命令, 打开 DNS 管理控制器, 可以看到如图 3-7 所示的图片, 以验证安装是否成功。

(6) 更改 DNS 服务器主机名, 并且为服务器添加后缀。为了后面的资源记录操作不出现异常, 我们最好在此处将服务器的主机名修改为规划的名字, 并且将这台服务器加入一个区域。

更改的方法如图 3-8 所示。首先在“系统属性”对话框内单击“更改”按钮, 然后在弹出的“计算机名/域更改”对话框内将规划的服务器主机名 dns 写入“计算机名”文本框内, 接着再单击“其他”按钮, 打开“DNS 后缀和 NetBIOS 计算机名”对话框, 最后在“此计算机的主 DNS 后缀”文本框内输入区域名称 jsigroup.cn, 单击“确定”按钮, 保存修改并重启系统使配置生效。

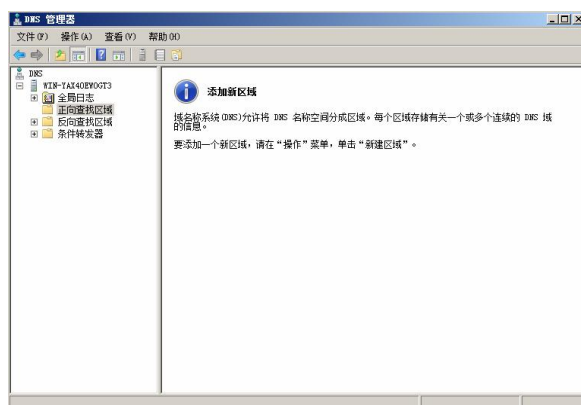


图 3-7 DNS 管理器

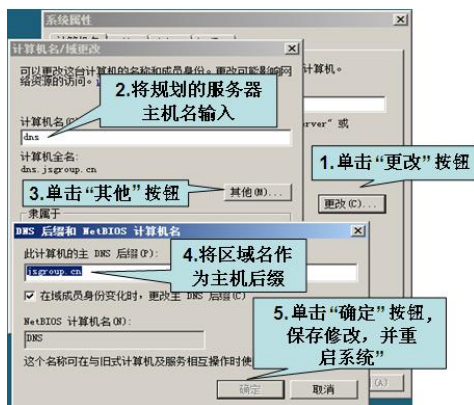


图 3-8 更改服务器主机名以及增加后缀

2. 创建 DNS 服务器区域

安装好 DNS 服务器之后, 就需要在服务器上创建区域文件。DNS 服务器的解析有正向解析和反向解析两种方式, 用于完成域名与 IP 地址的相互解析。正向解析需要创建正向查找区域, 反向解析需要创建反向查找区域。因此服务器的区域文件也需要根据需求进行正向区域和反向区域的创建。注意, 正向查找区域是必须建立的, 反向查找区域须在正向查找区域建立之后, 根据需求来决定是否创建。

(1) 正向查找区域的创建。

首先我们来创建完成正向地址解析的正向查找区域, 配置步骤如下:

1) 新建区域: 在“DNS 管理器”对话框中右击“正向查找区域”选项, 在弹出的菜单中选择“新建区域”选项, 如图 3-9 所示;

2) 区域类型: 由于创建的 DNS 服务器是本区域的主要 DNS 服务器, 因此在新建区域向导中的区域类型内选择创建“主要区域”, 然后单击“下一步”按钮, 如图 3-10 所示;

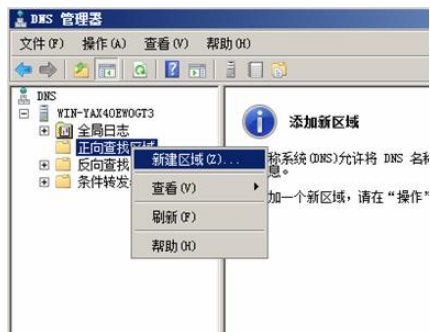


图 3-9 新建区域

3) 设置域名: 在新建区域向导中的“区域名称”对话框内输入获得的合法域名 jsgroup.cn, 如图 3-11 所示;

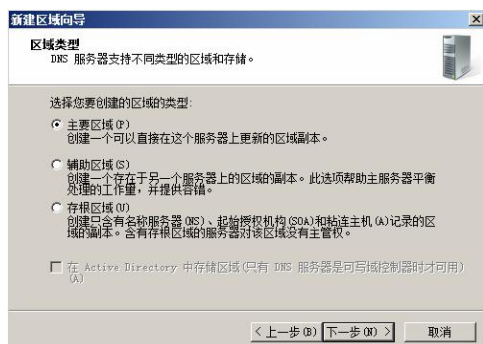


图 3-10 新建主要区域



图 3-11 设置区域名称

4) 创建区域文件: 在新建区域向导中的“区域文件”对话框内，系统为该区域文件设置了默认文件名，通常无须修改，单击“下一步”按钮即可，如图 3-12 所示;

5) 动态更新: 在新建区域向导中的“动态更新”对话框中可以选择不允许更新，一般来说，如果 DNS 区域在企业内网使用，我们会允许动态更新；如果用于 Internet，那么一般不需要动态更新，因此我们选择“不允许更新”单选项，如图 3-13 所示;

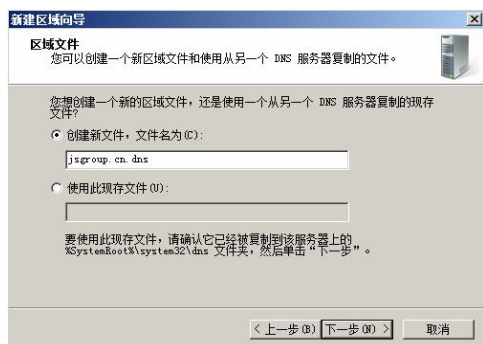


图 3-12 创建区域文件

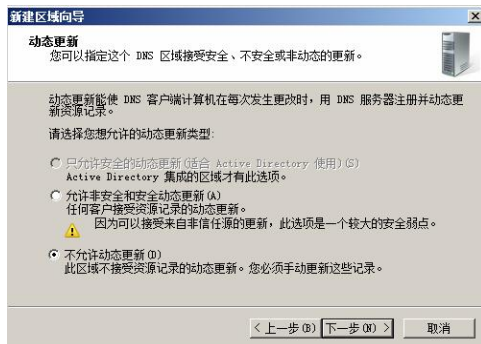


图 3-13 动态更新

6) 完成区域创建: 在新建区域向导中出现“正在完成新建区域向导”提示就说明正向查找区域即将安装完毕，单击“完成”按钮结束正向查找区域的创建。

通过以上步骤，在 DNS 管理器内可以看到“正向查找区域”下方已经出现了一个刚刚创建的区域 jsgroup.cn，说明正向查找区域创建完成，如图 3-14 所示。

(2) 反向查找区域的创建。

有时候我们也需要根据 IP 地址去查找域名，这种查询方式就是反向查询。反向查询需要建立反向查找区域，反向查找区域的配置步骤如下：

1) 新建区域: 在“DNS 管理器”对话框内右击“反向查找区域”选项, 在弹出的菜单中选择“新建区域”选项, 如图 3-15 所示;

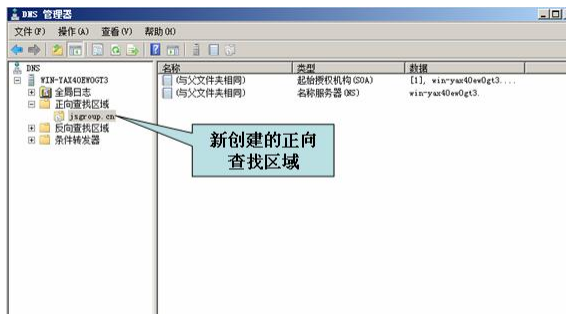


图 3-14 查看正向查找区域



图 3-15 新建反向查找区域

2) 区域类型: 打开新建区域向导, 单击“下一步”按钮, 进入区域类型, 选择“主要区域”;

3) 反向查找区域名称: 在新建区域向导中的“反向查找区域名称”对话框中选择“IPv4 反向查找区域”单选项, 如图 3-16 所示;

4) 网络 ID: 由于是反向地址解析区域, 因此需要设置用于解析的网络号。网络号是 IP 地址和子网掩码进行逻辑与运算后的结果, 反向区域的名称不能随便设置, 必须是颠倒的网络号再加上 in-addr.arpa 后缀。例如当前的网络号是 202.168.18, 那反向区域的名称就应该是 18.168.202.in-addr.arpa。本例中网络号应该是 202.168.10, 如图 3-17 所示。



图 3-16 反向查找区域名称

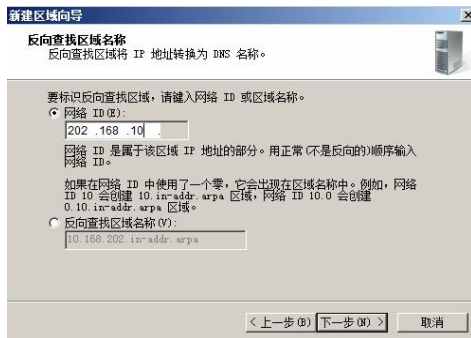


图 3-17 反向查找区域

5) 区域文件: 在新建区域向导中的“区域文件”对话框内, 可以保持默认的区域文件名, 单击“下一步”按钮;

6) 动态更新: 在新建区域向导中的“动态更新”对话框内设置“不允许动态更新”, 单击“下一步”按钮;

7) 完成区域创建: 单击“完成”按钮, 反向查询区域创建完毕, DNS 管理器对话框内“反向查找区域”内出现了刚创建的反向查找区域, 如图 3-18 所示。

3. 创建资源记录

DNS 记录是 DNS 区域数据的具体表现形式, DNS 的资源记录有 A、NS、SOA、MX、CNAME 和 PTR 记录等几种形式。创建何种资源记录类型是根据域名解析的需要来建立的。本案例中根据用户需求, 需要创建 A 记录(主机记录)、NS 记录(名称服务器记录)、SOA 记录(起始授权机构记录)、MX 记录(邮件交换记录)和 PTR 记录(指针记录)。以上几种记录的创建步骤如下。

(1) 创建 A 记录(主机记录)。

1) 打开“DNS 管理器”, 在正向查找区域内右击已经建立的区域名 jsigroup.cn, 在弹出来的菜单中选择“新建主机”选项, 如图 3-19 所示。

2) 在“新建主机”对话框中“名称”文本框输入网站服务器的主机名 www, “IP 地址”文本框内输入该服务器使用的 IP 地址 202.168.10.10。另外, 为了实现由 IP 地址到域名的反向域名解析, 需要创建 PTR 记录, PTR 记录可以在创建 A 记录(主机记录)的时候一并创建, 因此勾选“创建相关的指针(PTR)记录”复选框, 如图 3-20 所示。输入完毕, 单击“添加主机”按钮即可完成主机记录的创建。注意, 名称栏内仅输入服务器的主机名即可, 不要将后面的区域名录入;

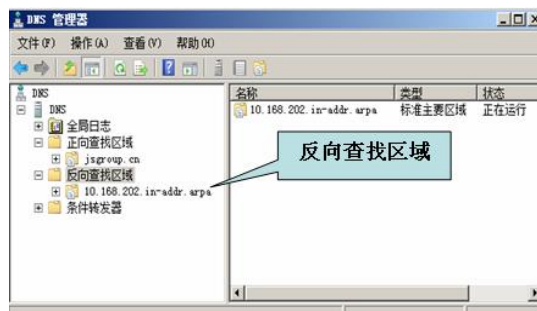


图 3-18 反向查找区域创建完毕



图 3-19 新建主机



图 3-20 创建主机记录

3) 弹出 DNS 确认对话框, 说明已经成功创建主机记录 www.jsigroup.cn, 单击“确定”按钮;
4) 按照同样的方法, 依次完成 FTP 服务器、OA 服务器和 Email 服务器的主机记录创建, 如图 3-21 所示。

(2) 创建 NS 记录(名称服务器记录)。

NS 记录用于说明这个区域有哪些 DNS 服务器负责解析, 因此 NS 记录是区域文件中不可

缺少的记录形式。在本区域 `jsgroup.cn` 中目前只规划有一台 DNS 服务器，因此仅建立一条 NS 记录即可，当然 NS 记录也离不开 A 记录为它提供解析，所以在创建 NS 记录之前，我们需要为 NS 记录创建一条 A 记录。配置步骤如下：

1) 在正向查找区域建立一条 A 记录，实现 DNS 服务器 `dns.jsgroup.cn` 到 IP 地址 `202.168.10.5` 的解析；

2) 右击正向区域 `jsgroup.cn`，在弹出的菜单中选择“属性”选项，打开属性对话框；

3) 在“`jsgroup.cn` 属性”对话框中选择“名称服务器”选项卡，如图 3-22 所示。

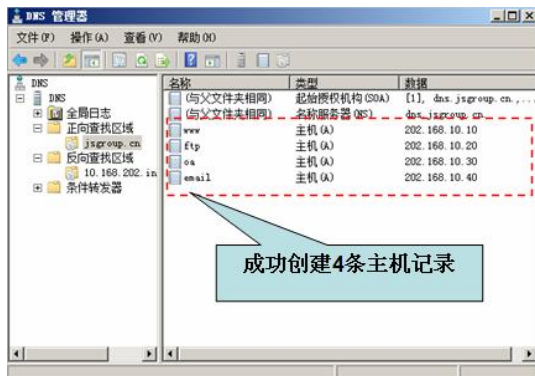


图 3-21 创建所需的主机记录

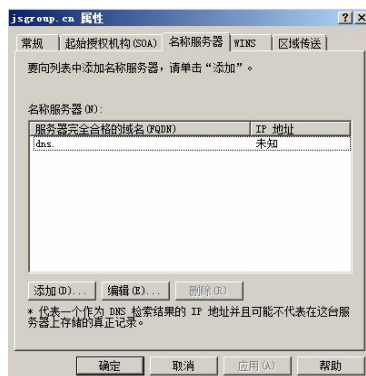


图 3-22 “`jsgroup.cn` 属性”对话框

4) 单击“编辑”按钮，打开“编辑 NS 记录”对话框。如果在图中“服务器完全合格域名”栏内出现的是域名是 `dns.`，那么这条系统自动建立的 NS 记录是有问题的，且不能正常工作，原因在于 `dns.` 并不是一个完全合格域名。我们需要修改 NS 记录，使它成为完全合格域名，因此我们将 `dns.` 修改为 `dns.jsgroup.cn.`（注意：CN 后的点不能缺少，这个点代表根域）。修改后的 NS 记录如图 3-23 所示。修改完全合格域名之后，在“此 NS 记录的 IP 地址”栏内输入 IP 地址 `202.168.10.5`。注意，如果修改前 NS 记录已经是一个完全合格域名，则无须修改。

(3) 创建 SOA 记录。

NS 记录说明了有哪些 DNS 服务器负责解析区域 `jsgroup.cn`，而 SOA 记录则进一步说明哪一个 DNS 服务器才是主服务器。SOA 记录也称为起始授权机构记录，负责说明哪个 DNS 服务器是主服务器，以及主服务器和辅助服务器之间的一些关联参数。因此对于一个 DNS 区域来说，NS 与 SOA 记录都是必不可少的记录。建立 SOA 记录的步骤如下：打开正向查找区域 `jsgroup.cn` 的属性对话框，单击“起始授权机构 (SOA)”选项卡。在该选项卡中的“主服务器”栏内出现的是 `dns.`。显然这个主服务器的完全合格域名也是有问题的，也同样需要修改。按照修改 NS 记录的方式将主服务器的名称改为完全合格域名，如图 3-24 所示。

(4) 创建 MX 记录。

创建 MX 记录的目的在于定位邮件服务器。要帮助找到邮件服务器，也必须首先为邮件服务器建立一条 A 记录，然后再创建 MX 记录。事先建立 A 记录的原因在于 MX 记录的描述

只包含完全合格域名，而不包含 IP 地址，所以只有通过 A 记录才能查到邮件服务器的位置。

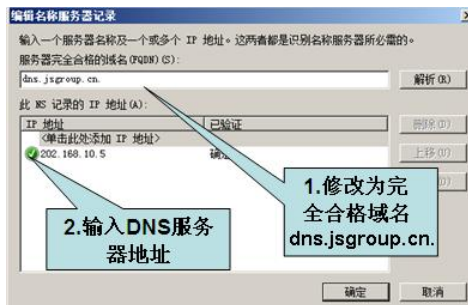


图 3-23 修改 NS 记录



图 3-24 修改 SOA 记录

MX 记录的配置步骤如下：

1) 为邮件服务器创建一条 A 记录：这一步已经在创建 A 记录的时候完成，如图 3-21 所示；

2) 在 DNS 管理器中右击正向查找区域 jsgroup.cn，在弹出的菜单中选择“新建邮件交换器 (MX)”选项，如图 3-25 所示；

3) 在“新建资源记录”对话框中，在“主机或子域”文本框内输入邮件服务器的主机名 email，在“邮件服务器的完全合格的域名”文本框内输入 email.jsgroup.cn，如图 3-26 所示。



图 3-25 新建邮件交换器

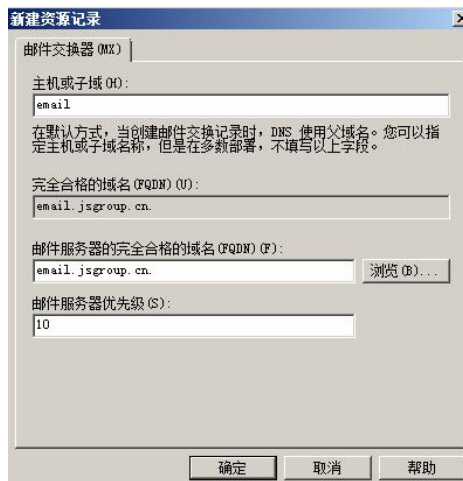


图 3-26 新建邮件交换记录

(5) 创建 PTR 记录。

PTR 记录也被称为指针记录，是 A 记录的逆向记录，作用是把 IP 地址解析为域名。PTR 记录的创建步骤如下：

1) 在 DNS 管理器中右击在“反向查找区域”下建立的反向区域 10.168.192.in-addr.arpa, 在弹出的菜单中选择“新建指针 (PTR)”选项, 如图 3-27 所示。

2) 在“新建资源记录”对话框中的“主机 IP 地址”文本框内输入网站服务器的 IP 地址 202.168.10.10, “主机名”文本框内输入主机的完全合格域名 www.jsgroup.cn., 如图 3-28 所示。



图 3-27 新建 PTR 指针



图 3-28 创建 PTR 记录

3) 按照同样的方法, 为 FTP 服务器、OA 服务器、EMAIL 服务器创建各自的 PTR 指针记录。创建完成之后如图 3-29 所示。

4. DNS 客户端的设置

DNS 服务器设置完成之后, DNS 客户端也需要设置, 才能为客户端主机进行 DNS 域名解析。DNS 客户端的设置相对简单, 只需要打开客户端主机的 IP 属性对话框, 在“首选 DNS 服务器”文本框中输入指定的 DNS 服务器 IP 地址即可, 如图 3-30 所示。



图 3-29 创建 FTP、OA 和 EMAIL 服务器的 PTR 指针记录



图 3-30 DNS 客户端设置

【任务验证】

完成以上配置后,为了验证 DNS 服务器是否可以域名解析,我们在客户端进行测试。

在任意一台客户端主机上打开命令对话框,输入指令 nslookup。在命令执行状态下,进行正向和反向地址解析,解析结果如图 3-31 所示。

```
> www.jsgroup.cn
Server:  Unknown
Address:  202.168.10.5

Name:     www.jsgroup.cn
Address:  202.168.10.10

> 202.168.10.10
Server:  Unknown
Address:  202.168.10.5

Name:     www.jsgroup.cn
Address:  202.168.10.10
```

(a) WWW 服务器的解析结果

```
> ftp.jsgroup.cn
Server:  Unknown
Address:  202.168.10.5

Name:     ftp.jsgroup.cn
Address:  202.168.10.20

> 202.168.10.20
Server:  Unknown
Address:  202.168.10.5

Name:     ftp.jsgroup.cn
Address:  202.168.10.20
```

(b) FTP 服务器的解析结果

```
> oa.jsgroup.cn
Server:  Unknown
Address:  202.168.10.5

Name:     oa.jsgroup.cn
Address:  202.168.10.30

> 202.168.10.30
Server:  Unknown
Address:  202.168.10.5

Name:     oa.jsgroup.cn
Address:  202.168.10.30
```

(c) OA 服务器的解析结果

```
> email.jsgroup.cn
Server:  Unknown
Address:  202.168.10.5

Name:     email.jsgroup.cn
Address:  202.168.10.40

> 202.168.10.40
Server:  Unknown
Address:  202.168.10.5

Name:     email.jsgroup.cn
Address:  202.168.10.40
```

(d) EMAIL 服务器的解析结果

图 3-31 解析结果

由图 3-31 可知,WWW 服务器、FTP 服务器、OA 服务器和 EMAIL 服务器的域名和对应 IP 地址均可以实现正向和反向地址解析,说明 DNS 服务器配置成功。

3.3 辅助 DNS 服务器配置

任务七 辅助 DNS 服务器规划

【任务描述】

为了避免因主 DNS 服务器故障带来的网络瘫痪,同时为了减轻正常工作的 DNS 服务器工作负担,需要在网络内另外创建一台 DNS 服务器作为辅助 DNS 服务器。

【任务要求】

1. 规划辅助 DNS 服务器 IP 地址。
2. 设置主、从 DNS 服务器区域文件数据同步方式。

【实施方法】

1. 设置辅助 DNS 服务器 IP 属性

根据前期的网络规划，为辅助 DNS 服务器指定相关参数如下：

主机名：dns2.jsgroup.cn

IP 地址：192.168.10.6/24

2. 设置主、从服务器数据同步方式

主 DNS 服务器保存着区域的所有文件记录，辅助服务器定期与主服务器进行同步，从主服务器那里复制区域文件到本服务器上。但出于安全原因，主服务器并不允许任意的 DNS 服务器从自己的区域中复制数据。在本任务中，为了实现安全的数据同步，我们设置同步方式为“仅允许本区域的服务器有复制权限”。

任务八 辅助 DNS 服务器配置

【任务描述】

设置辅助 DNS 服务器，实现域名解析的冗余备份和负载均衡功能

【任务要求】

- 1. 设置主服务器允许从服务器复制区域文件。
- 2. 创建辅助 DNS 服务器的正反向区域。
- 3. 辅助 DNS 服务器与主 DNS 服务器实现数据同步。

【实施方法】

1. 主 DNS 服务器配置

（1）主 DNS 服务器在正向和反向区域中各自增加一条 A 记录（主机记录），实现辅助服务器域名 dns2.jsgroup.cn 到 202.168.10.6 的正向和反向解析；

（2）打开主服务器正向查找区域“jsgroup.cn”的属性对话框，单击“名称服务器”选项卡，然后单击“添加”按钮；

（3）打开“新建名称服务器记录”对话框，在“服务器完全合格的域名”文本框内输入辅助服务器的完全合格域名 dns2.jsgroup.cn，再单击“解析”按钮，将该域名对应的 IP 地址自动解析到下面的“此 NS 记录的 IP 地址”栏内，如图 3-32 所示。如果未解析成功，也可以手动把 IP 地址输入到该栏目下；

（4）在主 DNS 服务器的“jsgroup.cn”区域属性对话框内单击“区域传送”选项卡，在“允许区域传送”栏下方有三种情况允许区域数据被传输：到所有服务器、只有在“名称服务器”选项卡中列出的服务器、只允许到下列服务器。为

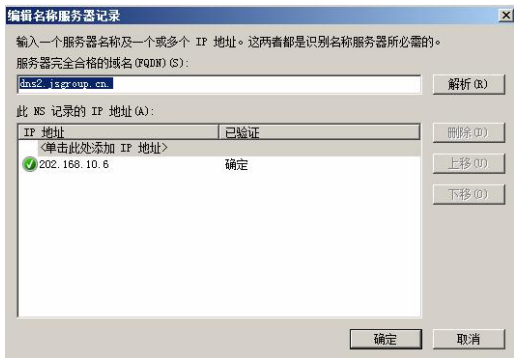


图 3-32 增加辅助服务器的一条 NS 记录

了安全,我们默认选择“只有在‘名称服务器’选项卡中列出的服务器”。如图 3-33 所示;

(5) 按照以上同样的方法,在反向区域中为辅助服务器增加一条 NS 记录,并且在“区域传送”选项卡中仅允许在名称服务器内的服务器复制文件。

2. 辅助 DNS 服务器的配置

(1) 选择一台专业服务器作为辅助 DNS 服务器的硬件平台,然后在服务器上面安装 Windows Server 2008 操作系统。再设置辅助 DNS 服务器的静态 IP 地址为 202.168.10.6/24;

(2) 在辅助 DNS 服务器上安装 DNS 组件,方法如前所述;

(3) 启动辅助服务器,修改辅助服务器的主机名,并将服务器加入区域 jsgroup.cn。修改重启之后,辅助服务器的完全合格域名为 dns2.jsgroup.cn.;

(4) 在辅助服务器上打开 DNS 管理器,右击“正向查找区域”选项,在弹出的菜单中选择“新建区域”命令;

(5) 在新建区域向导的区域类型中选择“辅助区域”,单击“下一步”按钮;

(6) 在新建区域向导的区域名称中输入区域名称 jsgroup.cn,单击“下一步”按钮;

(7) 在新建区域向导的“主服务器”栏内输入主 DNS 服务器 IP 地址 202.168.10.5,如图 3-34 所示。

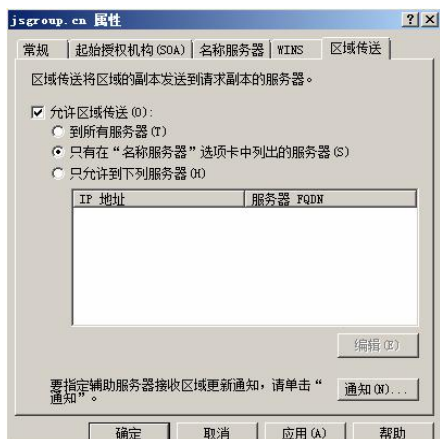


图 3-33 仅允许本区域服务器复制

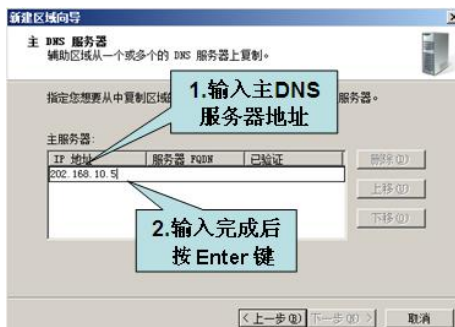


图 3-34 输入主 DNS 服务器地址

(8) 完成正向区域向导,右击重新打开 DNS 管理器的正向辅助区域,在弹出的菜单中选择“刷新”选项,辅助服务器即与主服务器进行同步,稍微等待一会就可以看到辅助服务器右侧窗口内也出现了与主服务器相同的记录,如图 3-35 所示。注意,如果出现数据传送故障,会显示故障信息“不是 DNS 服务器加载的区域”。这类故障是 DNS 区域复制的常见问题,主要是由于 DNS 辅助区域没有来得及与主服务器同步。只要稍微等待几分钟,再刷新一下区域即可恢复正常。

(9) 创建反向辅助查找区域,完成之后也同样与主服务器进行同步,如图 3-36 所示。



图 3-35 辅助服务器正向区域与主服务器同步



图 3-36 辅助服务器反向区域与主服务器同步

3. DNS 客户端的设置

由于采用了 DNS 辅助服务器，因此我们也需要在客户端 IP 属性内增加一个备用 DNS 服务器地址 202.168.10.6，如图 3-37 所示。



图 3-37 DNS 客户端设置

【任务验证】

1. 在主从 DNS 服务器都可以正常工作的时候,在客户端主机上运行 `nslookup` 指令进行测试,结果如图 3-38 所示。从图中可知,完成域名正反向解析的是主 DNS 服务器。

2. 关闭主服务器,模拟主服务器故障的情形,再次在客户端上运行 `nslookup` 指令进行测试。结果如图 3-39 所示,从图中可以看到,主 DNS 服务器已经无法联系,因此启用辅助 DNS 服务器,并且辅助服务器也同样完成了域名的正反向解析任务,实现了 DNS 解析的冗余功能。

```
Default Server: Unknown
Address: 202.168.10.5

> www.jsgroup.cn
Server: Unknown
Address: 202.168.10.5

Name: www.jsgroup.cn
Address: 202.168.10.10

> 202.168.10.10
Server: Unknown
Address: 202.168.10.5

Name: www.jsgroup.cn
Address: 202.168.10.10
```

图 3-38 主服务器解析

```
C:\Documents and Settings\Administrator>nslookup
*** Can't find server name for address 202.168.10.5: Non-existent domain
Default Server: dns2.jsgroup.cn
Address: 202.168.10.6

> www.jsgroup.cn
Server: dns2.jsgroup.cn
Address: 202.168.10.6

Name: www.jsgroup.cn
Address: 202.168.10.10

> 202.168.10.10
Server: dns2.jsgroup.cn
Address: 202.168.10.6

Name: www.jsgroup.cn
Address: 202.168.10.10
```

主服务器
无法联系

当前使用的是辅助
DNS服务器

图 3-39 辅助 DNS 服务器解析

3.4 DNS 子域和委派配置

任务九 DNS 子域和委派部署规划

【任务描述】

JSGroup 集团公司由于业务发展的需要,需要在全国各大城市建立分公司,扩展公司在行业的影响力和市场占有率。目前已经在成都和南京建立了分公司,并且南京分公司也准备建立自己的内部局域网,规划的域名是 `nanjing.jsgroup.cn`,成都子公司规划的域名为 `chengdu.jsgroup.cn`。两个子公司的网络通过互联网和总公司网络进行连接,但是由于没有为子公司网络规划 DNS 服务器,因此子公司的域名解析仍由总公司的 DNS 服务器来完成。这种方式显然并不合理,不仅加重了总公司 DNS 服务器的工作负担,而且来自南京本地的访问也需要到位于重庆的总公司来进行域名解析,数据传递花费的时间较长。因此针对这种现状,准备在南京子公司的网络内建立一台 DNS 服务器,将子公司的域名解析权限委派给子公司内的 DNS 服务器,这样既可以减轻总公司 DNS 服务器的工作负担,也可以提高解析速度,减少不必要的等待时间。但成都子公司考虑到设备成本和地理位置距离总公司较近,仍规划采用总公司的 DNS 服务器来解析域名。

【任务要求】

1. 规划公司网络拓扑结构图。
2. 规划成都和南京子公司网络域名。

3. 规划南京子公司的 DNS 服务器主机名。
4. 规划成都和南京子公司内需要解析的服务器域名及对应的 IP 地址。

【实现方法】

1. 公司网络拓扑结构设计

根据规划，该公司的网络拓扑结构如图 3-40 所示。

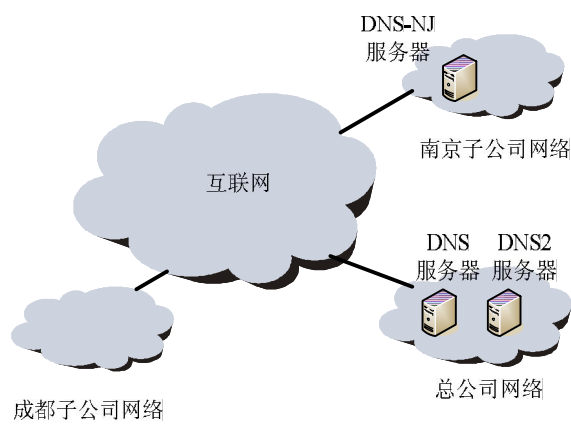


图 3-40 网络规划拓扑结构图

2. 成都、南京子公司的子域规划

对两个分公司所在的网络进行规划，如表 3-2 所示。

表 3-2 子域建设规划表

域名	子公司	DNS 服务器	IP 地址
Chengdu.jsgroup.cn	成都	dns.jsgroup.cn	202.168.10.5
		dns2.jsgroup.cn	202.168.10.6
Nanjing.jsgroup.cn	南京	dns-nj.jsgroup.cn	116.18.30.5

3. 分公司网络内服务器域名及 IP 规划

在两个分公司网络内部都设置了 Web、FTP 和 EMAIL 服务器。因此需要对这些使用域名建立对应的 DNS 映射。分公司网络内的服务器域名规划如表 3-3 所示。

表 3-3 域名解析规划表

子域名	需要解析的域名	对应的 IP 地址
Chengdu	www.chengdu.jsgroup.cn	202.168.20.10
	ftp.chengdu.jsgroup.cn	202.168.20.20
	email.chengdu.jsgroup.cn	202.168.20.30

续表

子域名	需要解析的域名	对应的 IP 地址
Nanjing	www.nanjing.jsgroup.cn	116.18.30.10
	ftp.nanjing.jsgroup.cn	116.18.30.20
	email.nanjing.jsgroup.cn	116.18.30.30

任务十 DNS 子域和委派部署规划

【任务描述】

设置成都和南京分公司的 DNS 子域，并将南京分公司子域的解析权限委派给南京子公司网络内的 DNS 服务器。

【任务要求】

- 1. 建立成都分公司的 DNS 子域。
- 2. 建立南京分公司的 DNS 子域。
- 3. 成都分公司的子域解析权限保留在总公司的 DNS 服务器。
- 4. 将南京子公司的子域解析权限委派给南京子公司的 DNS 服务器。
- 5. 在南京子公司的 DNS 服务器设置转发器。

【实施方法】

1. 成都子公司的子域创建

由于成都子公司的域名解析权仍在总公司的 DNS 服务器上，因此为成都子公司创建子域 chengdu.jsgroup.cn 的操作是在总公司的 DNS 服务器上进行的，配置步骤如下：

(1) 打开主 DNS 服务器的“DNS 管理器”窗口，右击正向查找区域的 jsgroup.cn，在弹出的菜单中选择“新建域”，如图 3-41 所示；

(2) 在“新建 DNS 域”对话框中输入成都子公司的子域名 chengdu，如图 3-42 所示；



图 3-41 新建子域



图 3-42 输入子域名称

(3) 在上图中单击“确定”按钮,子域创建完成,回到“DNS 管理器”窗口。可以在窗口左侧的树形目录下看到刚创建的子域 `chengdu.jsgroup.cn`。但子域视图中没有创建任何记录,如图 3-43 所示;

(4) 为了实现子域的反向查询功能,我们在反向查询区域也需要建立一个反向区域,右击“反向查找区域”选项,在弹出的菜单中选择“新建区域”命令,如图 3-44 所示;



图 3-43 子域创建成功



图 3-44 新建反向查找区域

(5) 在新建区域向导的“区域类型”中选择主要区域,然后选择“IPv4 区域”,在“反向区域名称”文本框内输入 `202.168.20`。完成反向区域的创建;

(6) 参照表 3-3,在子域视图内为成都子公司创建所需的主机记录和邮件交换记录,如图 3-45 所示。

2. 南京子公司的子域创建

南京子公司的子域域名 `nanjing.jsgroup.cn` 的解析方式与成都子公司不同,南京子公司需要单独配置一台 DNS 服务器负责解析南京子公司的子域名。因此配置步骤如下:

(1) 在总公司的主 DNS 服务器上配置委派。

1) 在“DNS 管理器”窗口内单击区域 `jsgroup.cn`,在弹出的菜单中选择“新建主机”命令,为被委派的主机 `dns-nj.jsgroup.cn` 建立一条主机记录,如图 3-46 所示;

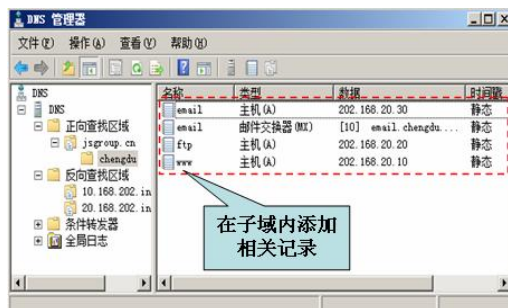


图 3-45 创建成都子域内的相关记录

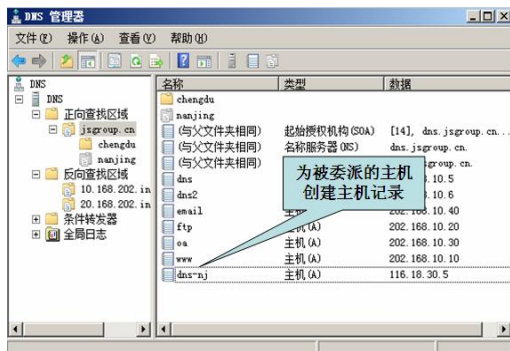


图 3-46 为被委派主机创建主机记录

2) 在“DNS 管理器”窗口内右击正向区域 jsgroup.cn, 在弹出的菜单中选择“新建委派”命令, 如图 3-47 所示;

3) 在新建委派向导的“受委派域名”对话框内输入南京子公司的子域名 nanjing, 如图 3-48 所示;

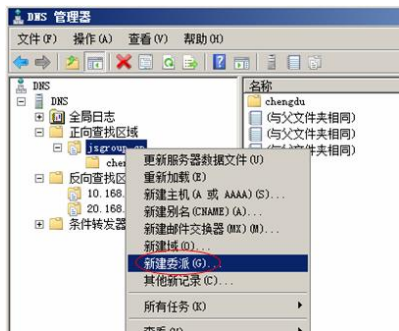


图 3-47 新建委派



图 3-48 受委派的子域名

4) 在新建委派向导的“名称服务器”对话框内指定用于子域 DNS 解析的服务器完全合格域名 dns-nj.nanjing.jsgroup.cn, 如图 3-49 所示。

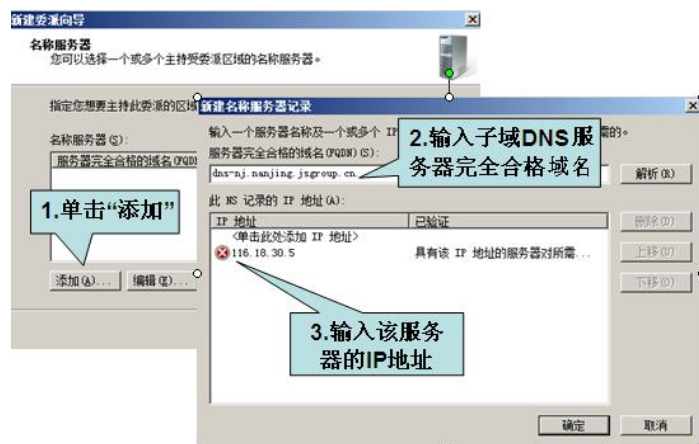


图 3-49 为委派指定名称服务器（即 NS 记录）

(2) 南京子公司 DNS 服务器配置。

子公司服务器配置之前, 先准备一台性能稳定的专业服务器, 并安装 Windows Server 2008 网络操作系统, 然后在服务器上设置静态 IP 地址 116.18.30.5, 将服务器的主机名改为 dns-nj, 并增加后缀 nanjing.jsgroup.cn, 使之成为子域 nanjing.jsgroup.cn 区域内的服务器。在子域服务器上的配置步骤如下:

1) 在服务器上安装 DNS 组件, 成为 DNS 服务器;

- 2) 在服务器上打开 DNS 管理器，右击正向查找区域，在弹出来的菜单中选择“新建区域”命令；
- 3) 在新建区域向导的“区域类型”对话框中选择“主要区域”，然后单击“下一步”按钮；
- 4) 在新建区域向导的“区域名称”对话框中输入区域名称 nanjing.jsgroup.cn，然后单击“下一步”按钮，如图 3-50 所示。
- 5) 在新建区域向导的“区域文件”对话框中，保留默认的区域文件名称及存放位置，单击“下一步”按钮；
- 6) 在新建区域向导的“动态更新”对话框中选择“不允许更新”单选项，单击“下一步”按钮；
- 7) 完成正向查找区域的创建，创建完成之后，可以看到该区域的视图中已经有了 SOA 记录和 NS 记录。检查 NS 记录，确保 NS 记录中服务器的名称为完全合格域名，并且该域名的 IP 地址正确；
- 8) 按照如前所述的方法为子域创建反向查找区域；
- 9) 创建完成正向和反向查找区域之后，刷新一下区域名称，则自动出现 DNS 服务器的主机记录（A 记录），然后再创建子域内的主机记录（即 WWW、FTP 和 EMAIL 服务器主机记录）和邮件交换记录，如图 3-51 所示。



图 3-50 子域的区域名称



图 3-51 子域服务器内的 A 记录和 MX 记录

- 10) 子域 DNS 服务器配置完毕之后，为了实现在子域服务器上也能查询总公司 jsgroup.cn 的域名，在子域服务器上设置条件转发器。在“DNS 管理器”窗口内右击“条件转发器”选项，在弹出来的菜单中选择“新建条件转发器”命令，如图 3-52 所示；
- 11) 在“新建条件转发器”对话框中的“DNS 域”栏内输入 jsgroup.cn，“主服务器的 IP 地址”栏内输入 202.168.10.5，再按 Enter 键确认，以完成条件转发器设置，如图 3-53 所示；

【任务验证】

1. 在主 DNS 服务器上运行 nslookup 指令，测试域名解析，结果如图 3-54 所示。

通过图示的默认服务器 IP 地址可知，负责解析的 DNS 服务器为 202.168.10.5。在区域 jsgroup.cn 内对本域的域名解析时，本服务器是作为权威服务器；而解析位于区域 nanjing.

jsgroup.cn 内的域名时，虽然也能得到解析结果，但这种解析是非权威解析（即本 DNS 服务器不是解析该域名的权威服务器），表明 DNS 区域委派功能成功实现。

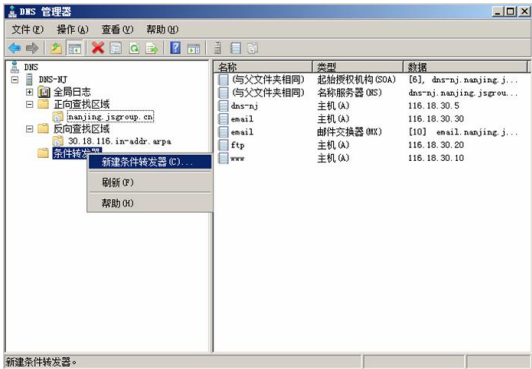


图 3-52 新建条件转发器

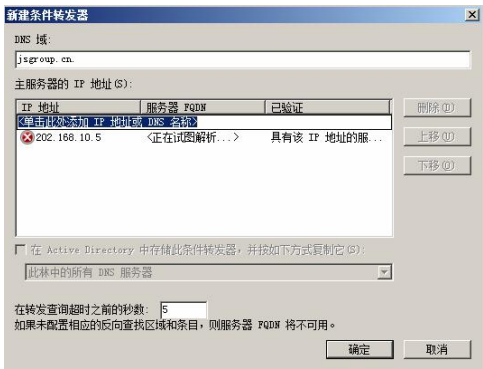


图 3-53 条件转发器设置

2. 在子域 DNS 服务器上运行 nslookup 指令，测试域名解析，结果如图 3-55 所示。



图 3-54 总公司域内 DNS 服务器测试解析域名



图 3-55 子公司域内 DNS 服务器测试解析域名

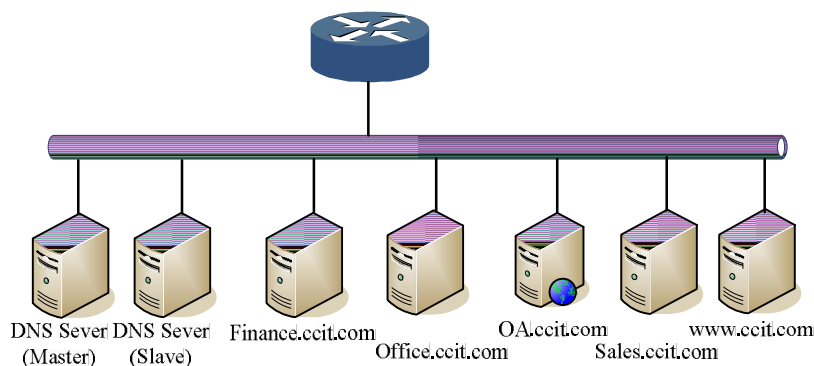
通过图示的默认服务器 IP 地址可知，负责解析的 DNS 服务器为 116.18.30.5。解析位于区域 jsgroup.cn 内的域名 www.jsgroup.cn 时，虽然也能得到解析结果，但这种解析是非权威解析（即本 DNS 服务器不是解析该域名的权威服务器，是通过转发器实现解析功能）；而在解析本区域 nanjing.jsgroup.cn 内的域名 www.nanjing.jsgroup.cn 解析时，本服务器是作为权威服务器。

3.5 综合实训

1. 综合实训 1

某企业有一个局域网（192.168.1.0/24），网络拓扑如下图所示。该企业中已经建立了 Web 服务器，员工希望通过域名来访问该服务器，同时员工也需要访问 Internet 上的网站。该企业已经申请了域名 ccit.com，公司需要 Internet 的用户通过域名访问公司的网页。为了保证可靠，

不能因为 DNS 的故障导致 Web 服务器不能访问。

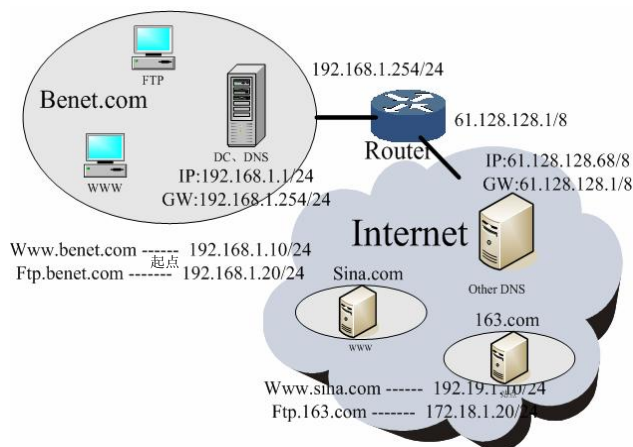


现要求在企业内部构建一台 DNS 服务器，为局域网中的计算机提供域名解析服务。DNS 服务器管理 ccit.com 域的域名解析，DNS 服务器的域名为 dns.ccit.com，IP 地址为 192.168.1.2/24。辅助 DNS 服务器的 IP 地址为 192.168.1.3/24。DNS 服务器同时还使用转发器为客户提供 Internet 上主机的域名解析，将外网的解析请求转发至公网 DNS 服务器（61.128.128.68）。要求分别能解析本区域内的以下域名：财务部（finance.ccit.com：192.168.1.11）、销售部（sales.ccit.com：192.168.1.12）、公司办公室（office.ccit.com：192.168.1.13）、OA 系统（oa.ccit.com：192.168.1.13）。

2. 综合实训 2

CNNET 公司有一台本地 DNS 服务器，IP 地址为 192.168.1.1 /24（区域名为 cnet.com）

建立本域内的主机记录 www.cnet.com 和 ftp.cnet.com，同时为 WWW 服务器建立一个别名 web.cnet.com。已知互联网上有一台 DNS 服务器（61.128.128.68），要求所有客户机能够解析本域内及互联网上的域名。实训拓扑图如下。



习题 3

一、选择题

1. DNS 区域有三种类型，分别是（ ）。
A. 标准辅助区域 B. 逆向解析区域
C. Active Directory 集成区域 D. 标准主要区域
2. 应用层 DNS 协议主要用于实现（ ）网络服务功能。
A. 网络设备名字到 IP 地址的映射 B. 网络硬件地址到 IP 地址的映射
C. 进程地址到 IP 地址的映射 D. 用户名到进程地址的映射
3. 测试 DNS 主要使用以下（ ）命令。
A. Ping B. IPconfig
C. nslookup D. Winipcfg

二、简答题

1. DNS 的查询方式有几种？简述其基本工作原理。
2. DNS 的区域类型有哪些？正向查询实现什么功能？反向查询实现什么功能？
3. 简述 nslookup 命令的使用方法。
4. DNS 主要区域与辅助区域各有什么作用？
5. DNS 服务器的资源记录主要有哪些？
6. DNS 服务器中转发器的功能是什么？